HUGH Q. COOK

March 13, 2001

124528
FAA-2000-7953-13

Docket Management System
U. S. Department of Transportation
Room Plaza 401
400 Seventh Street, S. W.
Washington, D.C. 20590

Dear Sir or Madam:

Please find attached my comments to NPRM FAA-2000-7953, Licensing and Safety Requirements for Launch.

Sincerely,

HQ Cook 3/13/01

Hugh Q. Cook

8513 FALCONET CIR., MC KINNEY, TX 75070
PHONE: 972-542-0425 • FAX: SAME, CALL FIRST

Review of NPRM FAA-2000-7953

OVERVIEW COMMENTS

The use of performance standards in lieu of explicit design requirements is, in general, good. The problem is that many hard-won painful lessons are imbedded in the detailed design requirements. Care should be taken to preserve detailed requirements where experience has shown they work better than most alternatives. Most engineers are cheerfully willing to comply with a detailed requirement, even when they don't understand it, as long as they know about it at the outset of a program. Trouble arises when an "unwritten rule" is imposed after all the tests are done. By publishing the explicit requirements in the Federal Register you alleviate the majority of the problems associated with explicit design requirements.

In a particularly important example, it is apparent that the regulations intend to abandon the requirement to use 1 amp/ 1 watt no-fire EEDs. This is one case where the use of performance based requirements is not as useful as a dictated design solution. There is no practical way to properly assess all possible permutations of the RF environment and the RF protection that hazardous EEDs live in. The military determined this after several fatal accidents. The best compromise is to define a minimum no-fire at a level low enough to allow reliable initiation, but high enough to account for unforeseen stray currents. The one amp standard has been shown empirically to satisfy this standard. D417.27(f) acknowledges the foregoing and encourages the launch operator to use 1amp/1 watt to satisfy the 20dB margin over stray electrical energy. An explicit requirement would save a lot of time and money.

The regulation requires that the launch operators affirm the information in the license, and sign an affidavit of sorts. A key point applies to flight safety analysis. Every analysis uses assumptions. Some of these assumptions are key to the analytic outcome. Often, empirical data is later developed that invalidates some key assumptions. An example is ISDS break-up analysis compared to structural load test results. Sometimes the vehicle doesn't break where you put the breakwires. A suggestion is to require the launch operator to clearly label key assumptions in analyses submitted for approval. At the Safety Review, a team could go through all key assumptions, and verify they are still valid.

There is no mention of the threat to the public caused by launch vehicle systems that create debris on orbit after the end of the mission. Pressurized systems are subjected to fatigue cycling on orbit due to thermal cycling. This fatigue has led to explosive failures of spent upper stages in the past. These explosions created massive amounts of debris, each with its own trajectory. There should be an explicit requirement for the de-pressurization of elements of the LV that achieve orbit, unless the licensee can prove that pieces couldn't possibly hit the space station.

There is no mention of LV operations creating a floating hazard to sea-going navigation. Its recently been discovered that Pegasus S1 survives impact and floats thousands of miles in the currents.

Compliance with the flight safety regulations can result in unexploded ordnance be disposed of in areas that are routinely visited by the general public. Booster stage flight termination destruct charges generally survive water impact. Booster stages generally impact in areas with relatively shallow sea floors. Sport scuba divers and bottom trawling commercial fishermen can be exposed to hazards related to these unexploded ordnance devices. This is probably in violation of some hazardous waste law. There should be some regulatory treatment of this issue.

There is no mention in the analysis instructions for computing casualties due to debris that take into account mass loss due to re-entry heating, and its effect on ballistic properties. This needs to be studied. Clearly there is some energy state where most of the item burns up prior to impact. It has an implication with respect to Africa overflight.

It should be explicitly stated that the reason a launch operator is the sole "responsible" party, and not the launch site operator, is to create a crystal clear allocation of liability should something go wrong. This is what is intended in the Act, and this is the basis for all the MPL activities.

In the discussion, you say that the FAA is not participating in an "operational" capacity, but you also require a "go" on the net. This makes FAA a de facto operational element. Launch operators must get FAA concurrence during the late countdown to launch, not unlike operations at a tower field.

Requiring launch operators to report **any** discrepancy may tend to generate too much paperwork. Some discrepancies are just too mundane to justify review by anybody but the manufacturer. Effort needs to be spent defining important characteristics that cannot be deviated from without concurrence up the chain. This is a common technique.

The FAA should look at the "TSO" program used for certifying safety critical aircraft avionics, and apply an analog to flight safety electronics.

In-flight safing of ISDS is where the flight software becomes safety critical. In the past, the ranges have not put much emphasis on software development standards for the flight software, and have relied on the launch operators running of dozens of simulated flight tests without inadvertent ISDS safing. While the software development standards published in 127-1 have been there for a few years, there will be a noticeable impact due to FAA enforcement of this part of the regulations.

SPECIFIC COMMENTS

Word omission in Discussion section D, page 63590, fifth paragraph, second sentence from end: ". . . is typically due to *these* three major hazards."

417.227(b)(6)(i) Using 31% as the failure rate for new launch vehicles seems low. A more appropriate and conservative figure would be 60% for the first flight or first flight after a major failure, then 30% for flights following successful flights up to 15.

415.127(d)(3) Drawings of flight safety component should show details of the mounting arrangements, since mounting arrangements influence environments that the components will see in flight.

417.117 (f)(6) The launch safety review is where all flight safety analyses are reviewed. Emphasis should be placed on reviewing the status of key assumptions.

417.205(d)(1) There is no reference to "steep" and "depressed" trajectories. The reference to maximum and minimum performance trajectories is a bit misleading. A hot, steep launch could have the same IIP trace characteristics as a low performing, nominally guided launch.

417.213(b)(4) Shouldn't FTS delay time be a factor in the offset of the flight safety limit from the flight control line?

417.221(d)(3) IIP *Cross* range rate is the parameter of interest.

417.317(c) The regulations don't address the emerging technology of lithium ion batteries.

417.327 (i) The ordnance initiator simulator (pulse catcher) should be operational any time power is applied to the vehicle to catch unintentional initiation events.

D417.17(f) 500VDC is sufficient to perform an adequate workmanship screening of wire harnesses.

D417.19(b)(2) The regulation should acknowledge that sometimes multiple EEDs are fired simultaneously from a battery, and state the margin requirement with respect to "all EEDs fired simultaneously."

D417.21(f) & D417.25(a) The reference to "armed and *locked*" implies that S&As and interrupters will have a separate mechanical lock incorporated in their design. Is this an implied requirement? The Thiokol 2134A doesn't have a lock, and probably doesn't need a lock, due to its gear train, but the Pacific Scientific ISDS interrupter that flew on Conestoga also didn't have a separate lock, and probably did need one, due to its direct acting solenoid design.

D417.25(b) Typo: remain in the *armed* position

D417.27(c) The requirement that an EED "must not degrade after a continuous application of no fire energy" is ambiguous. The reliability of an EED will likely be

affected by the application of 1 amp for five minutes, although it usually will fire afterward.

D417.27(new) The normal part-to-part variation of the functional output of the initiator must be consistent with next assembly requirements. (wildly inconsistent detonators may successfully initiate an ordnance transfer assembly, but with unknown margin.)

D417.31(a) This requirement is too "design" specific. There are better ways to prevent inadvertent pulling of lanyards, like not hooking them up until close-out.

D417.27 (i) and D417.5 (h)(2) There is an inconsistency with respect to helium leak requirements.

E417.27(d)(3) EBW firing unit monitoring for corona. Maximum corona susceptibility is usually encountered at an intermediate altitude, like 150,000 ft. It is important to monitor the firing unit during thermal vacuum tests.

E417.31 Percussion Actuated Device testing. Some primers use explosives that are susceptible to sublimation in a vacuum. Consideration should be given to adding a vacuum stability test if the primer is not hermetically sealed.

E417.39(c) In addition to the typical end-tip gap testing, pressure sensitive ordnance transfer systems have a unique characteristic where ordnance material comes off of the inner diameter of the transfer tube assembly, creating interruptions in the propagating media. There needs to be a requirement addressing propagation reliability with respect to allowable bare spots.